

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-112494

(43)Date of publication of application : 23.04.1999

(51)Int.Cl.

H04L 9/32
G06F 13/00
G09C 1/00
H04N 5/91
// H04N 7/167

(21)Application number : 09-271547

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 03.10.1997

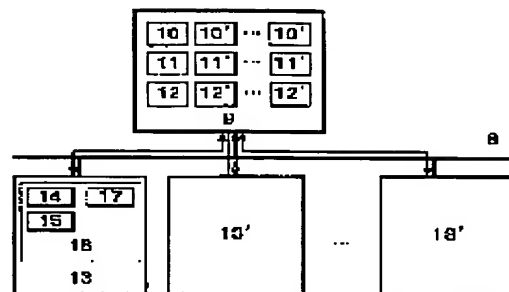
(72)Inventor : YAMAGUCHI TOMOHISA

(54) CLIENT/SERVER SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide high resistance against illegal copying by providing an illegal copying detect means for a client so as to detect illegal copying when illegal copying is tried in data cipher-released at the time of reproducing ciphered contents while dynamically releasing.

SOLUTION: At the client 13, a video reproducing application 16 executes an illegal copying detect module 17 and cipher releasing module 14. At the time of detecting illegal copying, the module 17 raises an illegal copying detect flag. Next, the application 16 checks the illegal copying detect flag. When the flag is raised, the execution of the module 14 is immediately finished and information on the detection of illegal copying is given to a video server 9. When the flag is not raised, ciphered video data 11 sent from the server 9 is cipher-released.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-112494

(43) 公開日 平成11年(1999) 4月23日

(51) Int.Cl.⁶
H 0 4 L 9/32
G 0 6 F 13/00
G 0 9 C 1/00
H 0 4 N 5/91
// H 0 4 N 7/167

識別記号

3 5 1
6 6 0

F I

H 0 4 L 9/00 6 7 1
G 0 6 F 13/00 3 5 1 Z
G 0 9 C 1/00 6 6 0 E
H 0 4 N 5/91 P
7/167 Z

審査請求 未請求 請求項の数11 O L (全 12 頁)

(21) 出願番号 特願平9-271547

(22) 出願日 平成9年(1997)10月3日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 山口 智久

東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

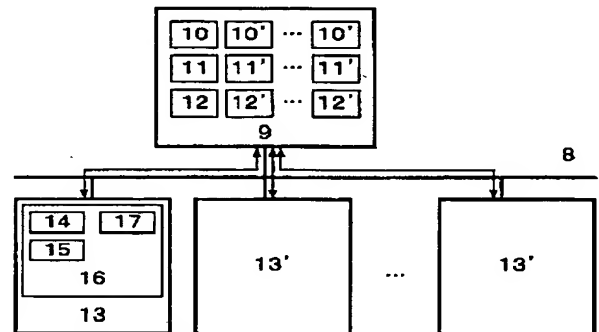
(74) 代理人 弁理士 宮田 金雄 (外2名)

(54) 【発明の名称】 クライアント・サーバシステム

(57) 【要約】

【課題】 クライアントに不正コピー検出機能を設け、不正コピーに対して高い耐性を持たせることを目的とする。

【解決手段】 ネットワークに接続されたサーバとクライアントからなるクライアント・サーバシステムにおいて、クライアントに不正コピー検出機能を設け、サーバから送られてくる暗号化コンテンツをクライアントで暗合を動的に解除しつつ再生する際において、暗合解除されたデータの不正コピーが試みられた場合に、不正コピー検出機能により不正コピーを検出し、不正コピーを防止するようにした。



【特許請求の範囲】

【請求項1】 ネットワークによって接続されたクライアント・サーバシステムにおいて、クライアントはサーバから転送されてきた暗号化されたコンテンツを解除する暗号解除手段と、

不正コピー検出手段を備え、

該不正コピー検出手段は、暗号化されたコンテンツを上記暗号解除手段で動的に解除しつつ再生する際に暗号解除されたデータに不正コピーが試みられていた場合に、不正コピーを検出することを特徴とするクライアント・サーバシステム。

【請求項2】 上記不正コピー検出手段は、データに不正コピーが試みられたことを検出した場合、暗号解除を中止することを特徴とする請求項1記載のクライアント・サーバシステム。

【請求項3】 上記不正コピー検出手段は、データに不正コピーが試みられたことを検出した場合、不正コピーが試みられた旨をサーバに通知することを特徴とする請求項1記載のクライアント・サーバシステム。

【請求項4】 上記不正コピー検出手段は、データに不正コピーが試みられたことを検出すると、不正コピーの内容とユーザ情報をサーバに通知することを特徴とする請求項1記載のクライアント・サーバシステム。

【請求項5】 サーバに不正コピーが試みられたこと、または不正コピーの内容とユーザ情報が上記サーバに通知された場合、サーバはクライアントに対する暗号化コンテンツの配信を中止することを特徴とする請求項3または請求項4記載のクライアント・サーバシステム。

【請求項6】 ネットワークによって接続されたクライアント・サーバシステムにおいて、

サーバはビデオカメラから取り込んだビデオデータをリアルタイムにエンコードしながら暗号化を行う暗号化手段を備え、

クライアントはサーバから転送されてきた暗号化されたビデオデータを解除する暗号解除手段と、

不正コピー検出手段を備え、

該不正コピー検出手段は、サーバから送られてきた暗号化されたビデオデータを動的に暗号解除しつつ再生する際に、暗号解除されたビデオデータに不正コピーが試みられていた場合に、不正コピーを検出することを特徴とするクライアント・サーバシステム。

【請求項7】 上記不正コピー検出手段は不正コピーが試みられたことを検出した場合、暗号解除を中止することを特徴とする請求項6記載のクライアント・サーバシステム。

【請求項8】 上記不正コピー検出手段は不正コピーが試みられたことを検出した場合、不正コピーが試みられた旨をサーバに通知することを特徴とする請求項6記載のクライアント・サーバシステム。

【請求項9】 上記不正コピー検出手段は不正コピーが

試みられたことを検出した場合、不正コピーの内容とユーザ情報をサーバに通知することを特徴とする請求項6記載のクライアント・サーバシステム。

【請求項10】 サーバに不正コピーが試みられたこと、または不正コピーの内容とユーザ情報が上記サーバに通知された場合、サーバはクライアントに対する暗号化コンテンツの配信を中止することを特徴とする請求項8または請求項9記載のクライアント・サーバシステム。

【請求項11】 ネットワークによって接続されたクライアント・サーバシステムにおいて、

サーバはユーザ情報として暗号化コンテンツ利用権情報を保持し、

クライアントがコンテンツ利用権を有していないコンテンツにアクセスした場合、暗号化されたコンテンツの一部分に対応した暗号化されていない部分コンテンツを配信することを特徴とするクライアント・サーバシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はネットワークによって接続されたクライアント・サーバシステムで暗号化されたコンテンツの利用に関する。

【0002】

【従来の技術】 ネットワークによって接続されたクライアント・サーバシステムにおいて、サーバに格納されている暗号化されたコンテンツをクライアントで暗号を動的に解除しつつ、再生処理を行う従来システムにおける構成を図11に示す。図11において、1はネットワーク、2は暗号化コンテンツ（暗号化されたコンテンツ）をネットワーク1を通して配信するサーバ、3はサーバ2に格納されている暗号化コンテンツデータである。また、4はネットワーク1を通して暗号化コンテンツを受信するクライアント、5はサーバ2から送られてきた暗号化コンテンツデータの暗号解除を動的に行う暗号解除モジュール、6は暗号解除モジュール5で暗号解除した暗号化コンテンツデータのデコードを行うデコードモジュール、7は暗号化コンテンツの再生を行うコンテンツ再生アプリケーションである。

【0003】 サーバ2はクライアント4上のコンテンツ再生アプリケーション7からの配信要求により暗号化コンテンツデータ3をネットワーク1を通して配信する。コンテンツ再生アプリケーション7は、クライアント4に送られてきた暗号化コンテンツデータ3を暗号解除モジュール5、デコードモジュール6を使用して再生処理を行う。

【0004】

【発明が解決しようとする課題】 従来のクライアント・サーバシステムは、以上のようにして構成されていたので、暗号解除モジュール5で暗号解除した暗号化コンテ

ンツデータが、フック機能等を使用され、不正コピーされてしまう可能性があった。

【0005】本発明は以上のような問題を解決するためになされたもので、クライアントに不正コピー検出機能を設け、不正コピーに対し高い耐性を有したクライアント・サーバシステムを提供することを目的とする。

【0006】

【課題を解決するための手段】第1の発明は、ネットワークによって接続されたクライアント・サーバシステムにおいて、クライアントはサーバから転送されてきた暗号化されたコンテンツを解除する暗号解除手段と、不正コピー検出手段を備え、該不正コピー検出手段は、暗号化されたコンテンツを上記暗号解除手段で動的に解除しつつ再生する際に暗号解除されたデータに不正コピーが試みられていた場合に、不正コピーを検出するようにしたものである。

【0007】第2の発明は、第1の発明に係わるクライアント・サーバシステムにおいて、不正コピー検出手段は、データに不正コピーが試みられたことを検出した場合、暗号解除を中止するようにしたものである。

【0008】第3の発明は、第1の発明に係わるクライアント・サーバシステムにおいて、不正コピー検出手段は、データに不正コピーが試みられたことを検出した場合、不正コピーが試みられた旨をサーバに通知するようにしたものである。

【0009】第4の発明は、第1の発明に係わるクライアント・サーバシステムにおいて、不正コピー検出手段は、データに不正コピーが試みられたことを検出した場合、不正コピーの内容とユーザ情報をサーバに通知するようにしたものである。

【0010】第5の発明は、第3または第4の発明に係わるクライアント・サーバシステムにおいて、サーバに不正コピーが試みられたこと、または不正コピーの内容とユーザ情報が上記サーバに通知された場合、サーバはクライアントに対する暗号化コンテンツの配信を中止するようにしたものである。

【0011】第6の発明はネットワークによって接続されたクライアント・サーバシステムにおいて、サーバはビデオカメラから取り込んだビデオデータをリアルタイムにエンコードしながら暗号化を行う暗号化手段を備え、クライアントはサーバから転送されてきた暗号化されたビデオデータを解除する暗号解除手段と、不正コピー検出手段を備え、不正コピー検出手段は、サーバから送られてきた暗号化されたビデオデータを動的に暗号解除しつつ再生する際に、暗号解除されたビデオデータに不正コピーが試みられていた場合に、不正コピーを検出するようにしたものである。

【0012】第7の発明は、第6の発明に係わるクライアント・サーバシステムにおいて、不正コピー検出手段は不正コピーが試みられたことを検出した場合、暗号解

除を中止するようにしたものである。

【0013】第8の発明は、第6の発明に係わるクライアント・サーバシステムにおいて、不正コピー検出手段は不正コピーが試みられたことを検出した場合、不正コピーが試みられた旨をサーバに通知するようにしたものである。

【0014】第9の発明は、第6の発明に係わるクライアント・サーバシステムにおいて、不正コピー検出手段は不正コピーが試みられたことを検出した場合、不正コピーの内容とユーザ情報をサーバに通知するようにしたものである。

【0015】第10の発明は、第8または第9の発明に係わるクライアント・サーバシステムにおいて、サーバに不正コピーが試みられたこと、または不正コピーの内容とユーザ情報が上記サーバに通知された場合、サーバはクライアントに対する暗号化コンテンツの配信を中止するようにしたものである。

【0016】第11の発明はネットワークによって接続されたクライアント・サーバシステムにおいて、サーバはユーザ情報として暗号化コンテンツ利用権情報を保持し、クライアントがコンテンツ利用権を有していないコンテンツにアクセスした場合、暗号化されたコンテンツの一部分に対応した暗号化されていない部分コンテンツを配信するようにしたものである。

【0017】

【発明の実施の形態】

実施の形態1. 本発明の第1の実施形態について、図1乃至図6に基づいて説明する。図1は本実施形態におけるシステム構成図であり、図において、8はネットワーク、9はネットワーク8を通して通常ビデオ（暗号化されていないビデオ）または暗号化ビデオ（暗号化されたビデオ）を配信するビデオサーバ、10はユーザ情報、11は通常ビデオデータ、12は暗号化ビデオデータである。また、13はネットワーク8を通して通常ビデオまたは暗号化ビデオを受信するクライアント、14はビデオサーバ9から送られてきた暗号化ビデオデータの暗号解除を行う暗号解除モジュール、15はビデオサーバ9から送られてきた通常ビデオデータまたは暗号解除モジュール14で暗号解除したビデオデータのデコードを行うデコードモジュール、16はユーザ認証、鍵交換、ビデオ再生等を行うビデオ再生アプリケーション、17は暗号化ビデオの不正コピーの検出を行う不正コピー検出モジュールである。本実施形態ではコンテンツとしてビデオを扱っているが、オーディオ、動画、静止画、その他のコンテンツにも適用可能である。

【0018】次に動作について図2、図3、図4を用いて説明する。ここで、図2はビデオ再生処理のフローチャートを示し、図3、図4は各々、ビデオ再生処理のフローチャート中における鍵交換処理（ステップ13）、および暗号化ビデオ再生処理（ステップ14）の詳細フ

ローチャートを示したものである。

【0019】図2のビデオ再生処理フローチャートにおいて、まずビデオ再生アプリケーション16はユーザが本システムを利用出来るか否かの認証を行うために、ログインダイアログボックスを出し、ユーザ名とパスワードを入力させ、これをビデオサーバ9に送る(ステップ1)。ビデオサーバ9では登録してあるユーザ情報を使用し、送られてきたユーザ名とパスワードからユーザ認証を行い、結果を返す。クライアント13ではログインできた場合に限り(ステップ2)、以下の処理を実行することが出来る。次にビデオ再生アプリケーション16はユーザからの要求を待ち(ステップ3)、ビデオ再生要求があった場合(ステップ5)には、ビデオサーバ9にビデオのタイトル情報を要求する。ビデオサーバ9はクライアント13からの要求に従いビデオのタイトル情報を返す。ビデオ再生アプリケーション16は送られてきたビデオのタイトル情報より、ビデオサーバ9に格納されているビデオの一覧を表示し、ビデオ選択ダイアログボックスを出し、ユーザにビデオを選択させる(ステップ6)。本実施形態では説明を簡素化するために、ユーザからの要求はビデオ再生要求とビデオ再生終了要求およびアプリケーション終了要求のみについて記述する。次に選択されたビデオの情報をビデオサーバ9に問い合わせ、選択されたビデオが暗号化されているかをチェックする(ステップ7)。暗号化されていない場合は、通常通りにビデオ再生を行う(ステップ8、ステップ9)。一方暗号化されている場合はユーザ情報10をビデオサーバ9に問い合わせ、ユーザに暗号化ビデオ利用権利があるか否かをチェックする(ステップ10)。

【0020】ここで、ユーザ情報10の構造を図5に示す。ユーザ情報10はユーザ名、パスワード、暗号化ビデオ利用権利情報からなる。暗号化ビデオ利用権利情報には暗号化ビデオを利用できるか否かのみを示す情報を格納してもよいし、ビデオ毎に利用できるユーザのレベルを設定しておき、暗号化ビデオ利用権利情報にレベルを格納しておき、それを元に利用できるか否かの判定を行ってもよい。また、暗号化ビデオ利用権利情報にどのビデオを利用できるか、という情報を格納しておいてもよい。

【0021】暗号化ビデオ利用権利がない場合(ステップ11)、ビデオ再生アプリケーション16は再生できない旨を表示して、ビデオの再生を行わず、ユーザからの要求待ち状態に戻ってもよいし、また可能であればビデオの先頭の数秒間などの暗号化ビデオに対応する部分再生をしてもよい(ステップ12)。

【0022】図6に部分再生を行う場合のビデオの格納方法を示す。暗号化ビデオデータに対応する部分データは暗号化されていないので、通常に再生を行うことができ、鍵交換を行う必要もない。ここでは部分データは暗号化ビデオデータの実ファイル名の一部を変換したもの

を例として挙げたが、別ディレクトリの同一ファイル名を使用するなど他の方法を用いてもよい。

【0023】一方、暗号化ビデオ利用権利がある場合は、鍵交換処理を行う(ステップ13)。鍵交換処理のフローチャートを図3に示す。本実施形態では共通鍵、公開鍵、秘密鍵を使用し鍵交換処理を行う。これは一例であり、他の鍵交換方式を使用することも出来る。暗号化ビデオの暗号化は共通鍵を使用している。図3において、まずビデオ再生アプリケーション16は公開鍵と秘密鍵の生成を行う(ステップ31)。次にユーザ情報と生成された公開鍵をビデオサーバ9に送る(ステップ32)。一方、ビデオサーバ9は受け取ったユーザ情報から、再度ユーザ認証を行う(暗号化ビデオ利用権利もチェック)(ステップ22)。ユーザ認証に成功した場合(ステップ23)は受け取った公開鍵で暗号化ビデオの共通鍵を暗号化し(ステップ24)、ビデオ再生アプリケーション16に送る(ステップ25)。次にビデオ再生アプリケーション16は、ビデオサーバ9から送られてきた公開鍵で暗号化された共通鍵を秘密鍵で暗号解除し、鍵交換処理を終了する(ステップ34)。

【0024】次にビデオ再生アプリケーション16は暗号化ビデオ再生処理を行う。暗号化ビデオ再生処理のフローチャートを図4に示す。まずビデオ再生アプリケーション16は暗号解除を行う前に不正コピー検出モジュール17および暗号解除モジュール14を実行させる(ステップ41、ステップ42)。不正コピー検出モジュール17はビデオ再生アプリケーション16の別スレッドとして動作し、実行を終了するまで常に不正コピーの検出を行い(ステップ43)、もし不正コピーを検出した場合(ステップ44)には不正コピー検出フラグを立てる。不正コピーの検出方法は、関数のアドレスをチェックしたり、I/Oを監視することなどがあげられるが、他の方法を用いてもよい。次にビデオ再生アプリケーション16は不正コピー検出フラグをチェックする。フラグが立っていた場合は直ちに暗号解除モジュール14の実行を終了させ(ステップ45)、ビデオサーバ9に対して不正コピー検出を通知して(ステップ46)、終了する。一方フラグが立っていなかった場合には、ビデオサーバ9から送られてくる暗号化ビデオデータ11の暗号解除を行う(ステップ47)。次にこの暗号解除された暗号化ビデオデータ11のデコードを行い(ステップ48)、ビデオおよびオーディオの出力を行う(ステップ49)。これをビデオが終了またはユーザからのビデオ再生終了要求があるまで繰り返し(ステップ50)、暗号化ビデオの再生を行う。ビデオが終了した場合には直ちに暗号解除モジュール14の実行を終了して(ステップ51)、不要な不正コピーの機会をなくす。次にユーザからの要求を待ち、ビデオ再生要求があった場合には上記したようにビデオの再生を行い、アプリケーション終了要求があった場合にはビデオ再生アプリケ

ーション16を終了する。以上のようにビデオ再生処理を行う。

【0025】実施の形態2. 次に本発明の第2の実施形態について、図7乃至図10に基づいて説明する。図7は本実施形態におけるシステム構成図であり、図7において18はネットワーク、19はネットワーク18を通して暗号化ライブビデオ（暗号化されたライブビデオ）を配信するビデオサーバ、20はユーザ情報、21はビデオカメラ、22はビデオカメラ21から入力されたライブビデオをリアルタイムにエンコードするエンコードモジュール、23はエンコードモジュール22でエンコードされたライブビデオデータを動的に暗号化する暗号化モジュールである。また、24はネットワーク18を通して暗号化ライブビデオを受信するクライアント、25はビデオサーバ19から送られてきた暗号化ライブビデオデータの暗号解除を行う暗号解除モジュール、26は暗号解除モジュール25で暗号解除したライブビデオデータのデコードを行うデコードモジュール、27はユーザ認証、鍵交換、暗号化ライブビデオ再生等を行う暗号化ライブビデオ再生アプリケーション、28は暗号化ライブビデオの不正コピーの検出を行う不正コピー検出モジュールである。本実施形態ではコンテンツとしてライブビデオを扱っているが、ライブオーディオ、サーバに格納されているビデオ、オーディオ、動画、静止画その他のコンテンツにも適用可能である。

【0026】次に動作について、図8、図9を用いて説明する。図8はビデオサーバ19における暗号化ライブビデオ配信処理のフローチャートであり、図8(b)は図8(a)の暗号化ライブビデオ配信処理（ステップ75の詳細フローチャートである。また、図9はクライアント24における暗号化ライブビデオ再生処理のフローチャートである。まず図8において、ビデオサーバ19ではユーザ（クライアントのユーザではなく、サーバのユーザであり、管理者などである）からエンコード開始要求に従い（ステップ72）、ビデオカメラ21からのライブビデオデータをエンコードモジュール22でリアルタイムにエンコードする（ステップ73）。次に、このライブビデオデータを暗号化モジュール23で動的に暗号化する（ステップ74）。この状態でクライアントからの要求を待つ（ステップ80）。

【0027】一方、図9のクライアント24では暗号化ライブビデオ再生アプリケーション27がユーザが本システムを利用出来るかの認証を行うために、ログインダイアログボックスを出し、ユーザ名とパスワードを入力させ、これをビデオサーバ19に送る（ステップ59）。

【0028】すると、図8のビデオサーバ19では登録してあるユーザ情報20を使用し、送られてきたユーザ名とパスワードからユーザ認証を行い（ステップ81）、結果を返し、クライアントからの要求待ちにもど

る（ステップ80）。

【0029】クライアント24ではログインできた場合に限り（ステップ60）、以下の処理を実行することが出来る。暗号化ライブビデオ再生アプリケーション27はユーザからの要求を待ち（ステップ61）、暗号化ライブビデオ再生要求があった場合には（ステップ62）ビデオサーバ19にユーザ情報20をサーバに問い合わせ、サーバからのユーザ情報に基づいて（ステップ82）、ユーザが暗号化ライブビデオ利用権利があるかをチェックする（ステップ63）。

【0030】ユーザ情報20は実施形態1と同一のものを使用してもよいし、図10に示すように別途暗号化ライブビデオ利用権情報を保持するようにしてもよい。

【0031】暗号化ライブビデオ利用権利がない場合（ステップ64）、暗号化ライブビデオ再生アプリケーション27はライブビデオの再生が出来ない旨を表示して（ステップ65）ライブビデオを再生せず、ユーザからの要求待ち状態に戻る。一方、暗号化ライブビデオ利用権利がある場合は鍵交換処理を行う（ステップ66）。鍵交換処理は実施形態1と同様のものである（図3）。次にライブビデオ再生アプリケーション27は暗号化ライブビデオ再生処理を行う（ステップ67）。暗号化ライブビデオ再生処理は実施形態1と同様のものである（図4）。暗号化ライブビデオ再生処理の中で、不正コピーが試みられたことが不正コピー検出モジュール28で検出され、ビデオサーバ19に不正コピー検出通知があった場合（ステップ83）、ビデオサーバ19ではライブビデオのエンコード、暗号化、他のクライアントへの暗号化ライブビデオの配信は続行し、不正コピーが検出されたクライアントへの暗号化ライブビデオの配信のみを中止する。またマルチキャストで配信している場合には不正コピーが検出されたクライアントをメンバーからはずすことによって配信を中止する（ステップ84）。さらにビデオサーバ19ではクライアントから送られてきたユーザ情報、不正コピーの情報を履歴情報などに追加し、不正コピーの解析を行う（ステップ85）。以上のようにして、暗号化ライブビデオ再生／配信処理を行う。

【0032】

【発明の効果】第1の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出できるようにしたので、サーバに格納されている暗号化されたコンテンツをクライアントで暗号化解除する際に不正コピーに対する高い耐性を保持することができるという効果がある。

【0033】第2の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出すると、暗号解除を中止することができるようにしたので、サーバに格納されている暗号化コンテンツをクライアントで暗号化解除する際に不正コピーをクライアント側か

ら防止できるという効果がある。

【0034】第3の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出するとサーバに通知するようにしたので、サーバは格納されている暗号化コンテンツの配信を中止することができるという効果がある。

【0035】第4の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出すると、ユーザ情報と不正コピーの内容をサーバに通知するようにしたので、不正コピーに対するフィードバックや不正コピーユーザに対する対応措置が可能となる。

【0036】第5の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたり、不正コピーの内容とユーザ情報がサーバに通知されたときに、サーバはクライアントに対する暗号化コンテンツの配信を中止するようにしたので、不正コピーをサーバ側から防止できるという効果がある。

【0037】第6の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出できるようにしたので、サーバが動的に暗号化したコンテンツをクライアントで暗号化を解除する際に不正コピーに対する高い耐性を保持することができるという効果がある。

【0038】第7の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出すると暗号解除を中止するようにしたので、サーバが動的に暗号化したコンテンツをクライアントで暗号化解除する際に不正コピーをクライアント側から防止できるという効果がある。

【0039】第8の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことが直ちにサーバに通知されるので、サーバが動的に暗号化している暗号化コンテンツの配信を中止することができるという効果がある。

【0040】第9の発明に係わるクライアント・サーバシステムは、不正コピーが試みられたことを検出すると、ユーザ情報と不正コピーの内容をサーバに通知するようにしたので、不正コピーに対するフィードバックや不正コピーユーザに対する対応措置が可能となるという効果がある。

【0041】第10の発明に係わるクライアント・サーバシステムは、不正コピーが試みられるとサーバは動的に暗号化しているコンテンツの配信を中止するようにしたので、不正コピーをサーバ側から防止できるという効果がある。

【0042】第11の発明に係わるクライアント・サーバ

システムは、サーバに暗号化コンテンツ利用権情報を保持し、該コンテンツに対する利用権を所持していないユーザに対しても、暗号化されたコンテンツの1部に対するアクセスを可能としたので、暗号化コンテンツの1部分を試聴することができるという効果がある。

【図面の簡単な説明】

【図1】 本発明の第1の実施形態を示すシステム構成図である。

【図2】 本発明の第1の実施形態におけるビデオ再生処理のフローチャートを示す図である。

【図3】 本発明の第1および第2の実施形態における鍵交換処理のフローチャートを示す図である。

【図4】 本発明の第1および第2の実施形態における暗号化ビデオ及びライブビデオ再生処理のフローチャートを示す図である。

【図5】 本発明の第1の実施形態におけるユーザ情報の構造を示す図である。

【図6】 本発明の第1の実施形態における暗号化ビデオに対応する部分データの格納方式を示す図である。

【図7】 本発明の第2の実施形態を示すシステム構成図である。

【図8】 本発明の第2の実施形態のビデオサーバにおける暗号化ライブビデオ配信処理のフローチャートである。

【図9】 本発明の第2の実施形態のクライアントにおける暗号化ライブビデオ再生処理のフローチャート示す図である。

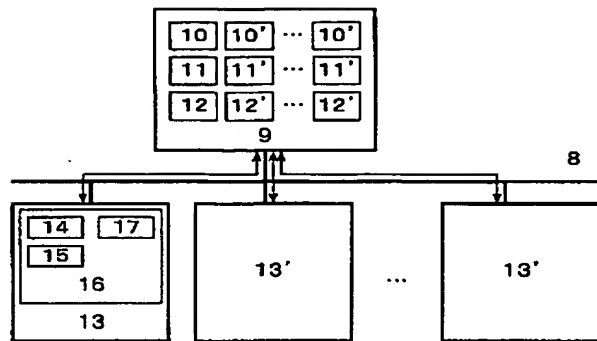
【図10】 本発明の第2の実施形態におけるユーザ情報の構造を示す図である。

【図11】 従来の暗号化コンテンツを配信するクライアント・サーバシステム構成図である。

【符号の説明】

1 ネットワーク、2 サーバ、3 暗号化データ、4 クライアント、5 暗号解除モジュール、6 デコードモジュール、7 暗号化コンテンツ再生アプリケーション、8 ネットワーク、9 ビデオサーバ、10 ユーザ情報、11 通常ビデオデータ、12 暗号化ビデオデータ、13 クライアント、14 暗号解除モジュール、15 デコードモジュール、16 ビデオ再生アプリケーション、17 不正コピー検出モジュール、18 ネットワーク、19 ビデオサーバ、20 ユーザ情報、21 ビデオカメラ、22 エンコードモジュール、23 暗号化モジュール、24 クライアント、25 暗号解除モジュール、26 デコードモジュール、27 暗号化ライブビデオ再生アプリケーション、28 不正コピー検出モジュール。

【図1】



【図5】

ユーザ情報	
ユーザ名	
パスワード	
暗号化ビデオ利用権利情報	

【図6】

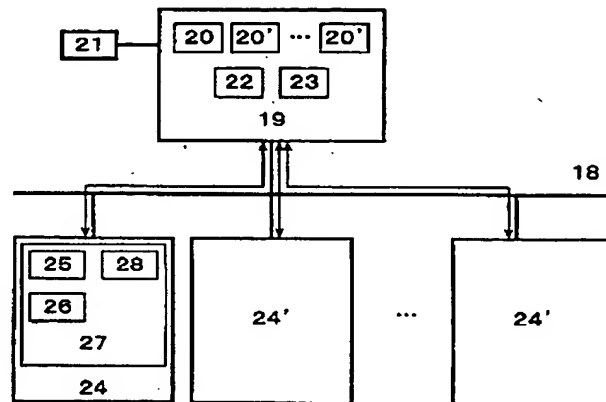
暗号化ビデオデータ

実ファイル名: xxxxxx.xxx

暗号化ビデオに対応する部分データ

実ファイル名: yxxxxxx.xxx

【図7】

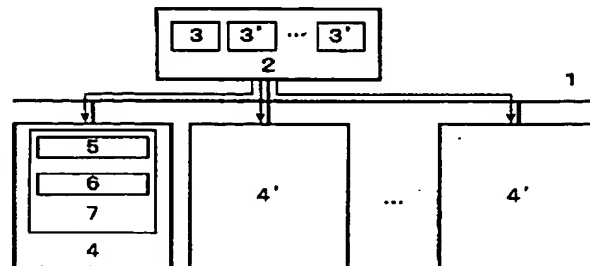


【図10】

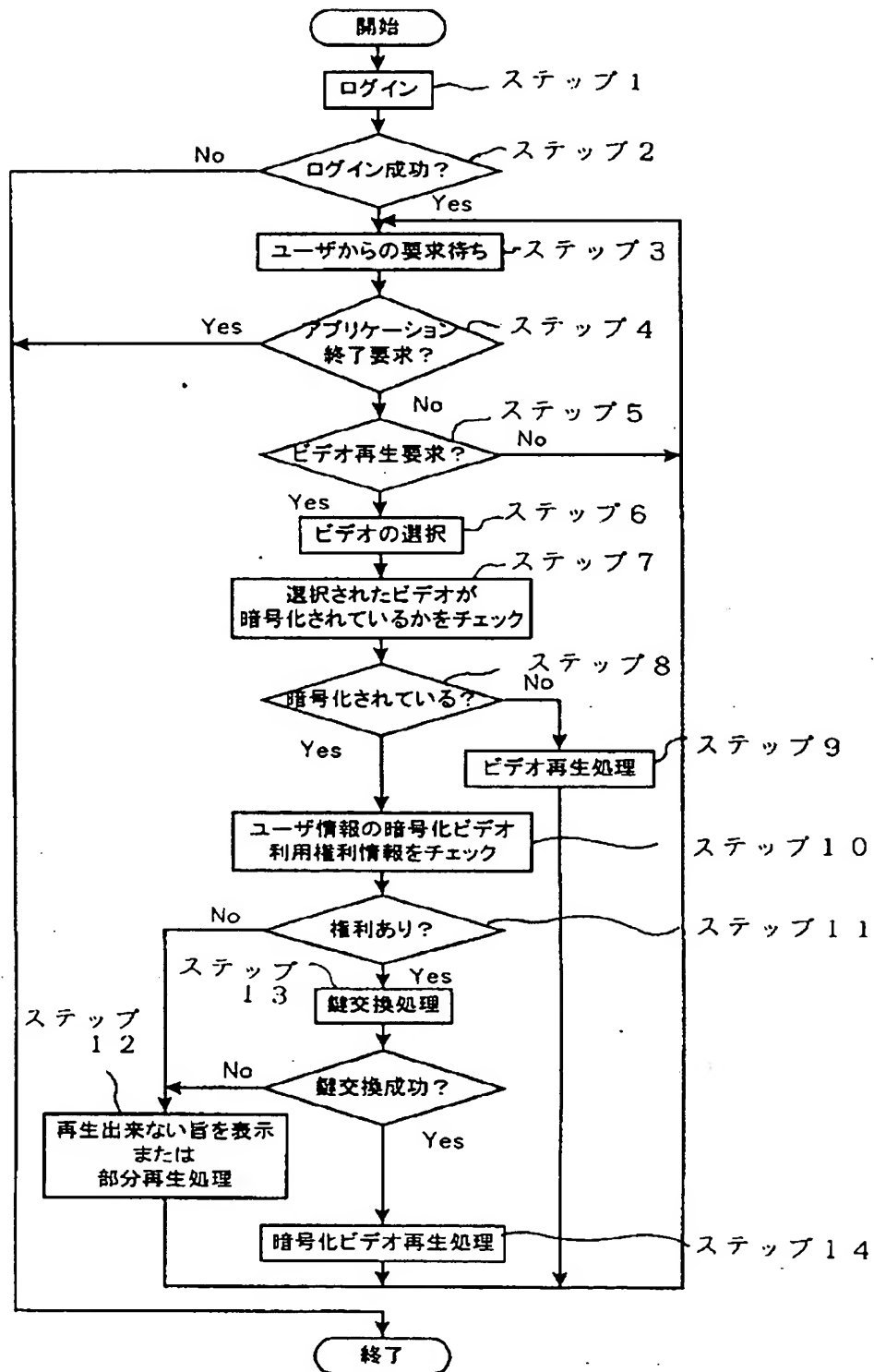
ユーザ情報

ユーザ名
パスワード
暗号化ビデオ利用権利情報
暗号化ライブビデオ利用権利情報

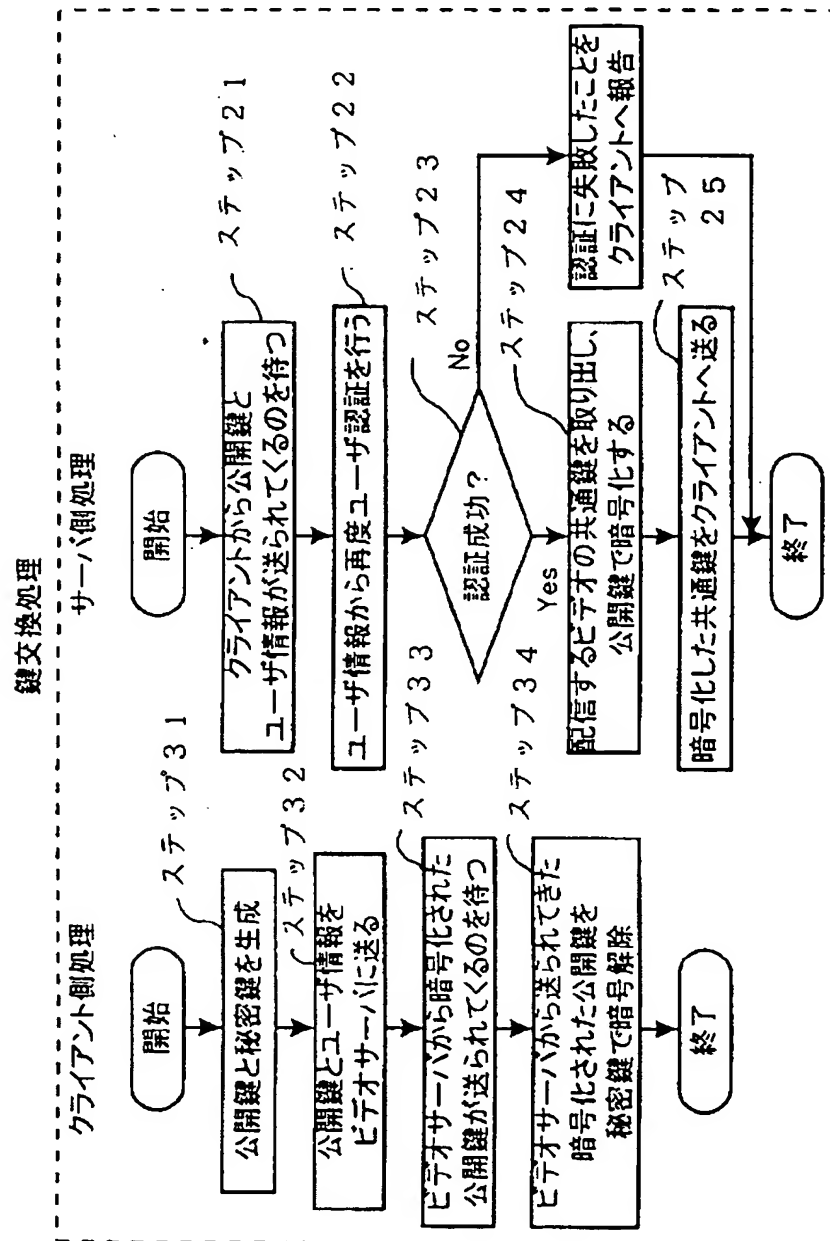
【図11】



【図2】

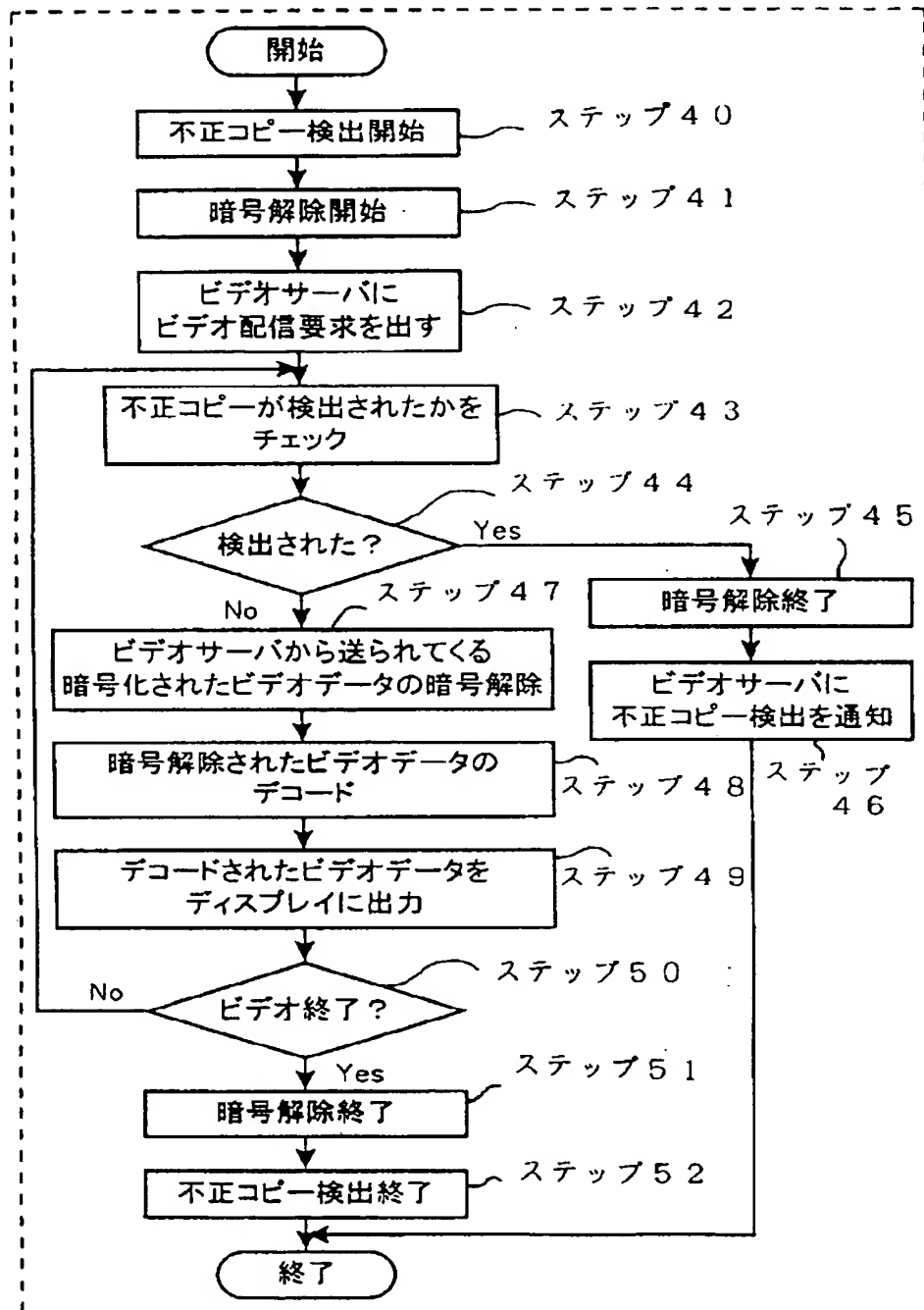


【図3】

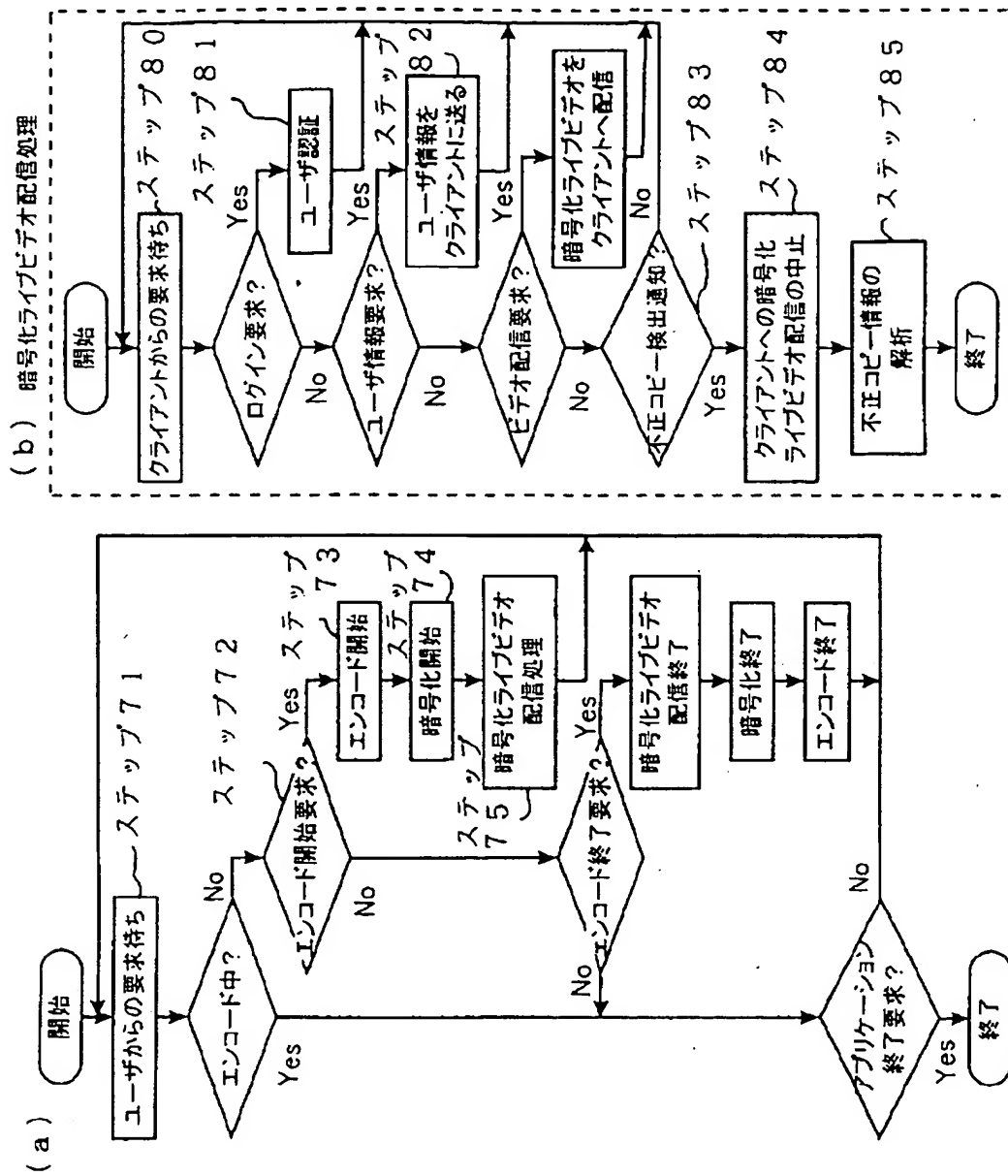


【図4】

暗号化ビデオ／ライブビデオ再生処理



【図8】



【図9】

